(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-244044
(P2006-244044A)
(43)公開日　平成18年9月14日(2006.9.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 3/12	(2006.01)	G06F	3/12	C	5B021
G06K 17/00	(2006.01)	G06F	3/12	K	5B058
		G06K	17/00	F	
		G06K	17/00	L	

審査請求 未請求　請求項の数 9　ＯＬ　（全 12 頁）

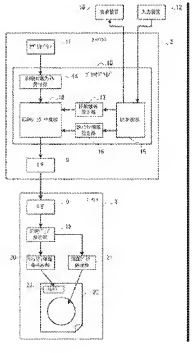
(21)出願番号　特願2005-57641(P2005-57641)
(22)出願日　平成17年3月2日(2005.3.2)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目１７番２２号
(74)代理人　100071054
弁理士　木村　高久
(72)発明者　萩中　孝則
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル
富士ゼロックス株式会社内

Ｆターム(参考)　5B021 AA04 CC05 LL06 NN18 NN19
QQ01 QQ07
5B058 CA15 KA31 YA20

(54)【発明の名称】文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタ

(57)【要約】
【課題】印刷物を紙１枚単位で持ち出しの制限を実施することで、文書等のセキュリティを高めることが可能な文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタを提供する。
【解決手段】入力装置によりセキュリティ情報および印刷情報を入力し、印刷ジョブ作成部はアプリケーションからの印刷対象ファイルに基づいて印刷ジョブを作成し、作成した印刷ジョブに対し、セキュリティ情報指定部がセキュリティ情報を設定するとともに印刷情報設定部が印刷情報を設定し、印刷ジョブをプリンタに送信し、プリンタの印刷ジョブ解析部は印刷ジョブを解析し、印刷ジョブ処理部は印刷情報に従って印刷対象ファイルの画像を用紙上に形成し、セキュリティ情報書込み部はセキュリティ情報を用紙に埋め込まれたＩＣタグに書き込む。
【選択図】図２



【特許請求の範囲】
【請求項１】
クライアント装置からの印刷ジョブに基づき、プリンタが印刷した文書の文書持出制限システムにおいて、
前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成する処理と、
前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定する処理と、
該設定した印刷ジョブを前記プリンタに送信する処理と
をクライアント装置に動作させるプリンクドライバと、
前記クライアント装置から受信した印刷ジョブを解析する印刷ジョブ解析手段と、
前記印刷ジョブ解析手段で解析した印刷ジョブに設定されたセキュリティ情報を、前記用紙に付加されたＩＣタグに書き込むセキュリティ情報書込み手段と、
前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを前記用紙に形成する印刷ジョブ処理手段と
を具備するプリンタと
を具備することを特徴とする文書持出制限システム。
【請求項２】
前記用紙に付加されたＩＣタグに書き込まれたセキュリティ情報を読み込むセキュリティ情報読込手段と、
前記セキュリティ情報読込手段で読み込んだセキュリティ情報に基づき、前記用紙が前記持出可能範囲への持出が許可されているか否か判定する判定手段と
を具備し、前記持出可能範囲の境界に設置された検出器
を更に具備することを特徴とする請求項１記載の文書持出制限システム。
【請求項３】
前記プリンタドライバは、
前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する処理
をクライアント装置に動作させることを特徴とする請求項１記載の文書持出制限システム。
【請求項４】
クライアント装置からの印刷ジョブに基づき、プリンクが印刷した文書の文書持出制限方法において、
前記クライアント装置のプリンタドライバは、
前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成し、
前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定し、
該設定した印刷ジョブを前記プリンタに送信し、
前記プリンタは、
前記クライアント装置から受信した印刷ジョブを解析し、
該解析した印刷ジョブに設定されたセキュリティ情報を、前記用紙に付加されたＩＣタグに書き込み、
該解析した印刷ジョブに含まれる印刷データを前記用紙に形成する
ことを特徴とする文書持出制限方法。
【請求項５】
前記持出可能範囲の境界に設置された検出器は、
前記用紙に付加されたＩＣタグに書き込まれたセキュリティ情報を読み込み、
該読み込んだセキュリティ情報に基づき、前記用紙が前記持出可能範囲への持出が許可されているか否か判定する
ことを特徴とする請求項４記載の文書持出制限方法。

【請求項6】
前記プリンタドライバは、
前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する
ことを特徴とする請求項４記載の文書持出制限方法。
【請求項7】
プリンタに送信する印刷ジョブを作成するクライアント装置にインストールされたプリンタドライバにおいて
前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成する処理と、
前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定する処理と、
該設定した印刷ジョブを前記プリンタに送信する処理と
をクライアント装置に動作させることを特徴とするプリンタドライバ。
【請求項8】
前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する処理
をクライアント装置に動作させることを特徴とする請求項７記載のプリンタドライバ。
【請求項9】
クライアント装置と接続するプリンタにおいて、
前記クライアント装置から受信した印刷ジョブを解析する印刷ジョブ解析手段と、
前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を、該用紙に付加されたＩＣタグに書き込むセキュリティ情報書込み手段と、
前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを前記用紙に形成する印刷ジョブ処理手段と
を具備することを特徴とするプリンタ。
【発明の詳細な説明】
【技術分野】
【0001】
本発明は、文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタに関し、特に、用紙に埋め込まれたＩＣタグの情報に基づいて文書の持ち出しを制限する文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタに関する。
【背景技術】
【0002】
近年、スーパーマーケット、百貨店、小売店等の店舗における商品の万引きまたは盗難を防止する目的で、それら商品の包装材に盗難防止用のＩＣタグ等が取り付けられることが多くなっている。
【0003】
この盗難防止用のＩＣタグは通常カード状を呈し、例えば、特定の周波数の電磁波に感応し、この電磁波と同一または異なる周波数の電磁波を発信し、著しくは磁性体により電磁場等の所定の場の変化を店舗の出口等で検知することにより万引きまたは盗難を防止するものである。
【0004】
例えば、ＩＣタグを利用して、ホテル、マンション等の内部を複数のエリアに分割された建物において、各エリアへの出入り管理を自動的に行うとともに、出入りにより各エリアに装備された照明施設、空調施設等を自動的に作動／停止することができる特定エリアへの出入りによるサービス提供システムがある（例えば、特許文献１参照。）。
【0005】
また、例えば、ＩＣタグを利用して、書籍、雑誌等の包装材料に情報の読書き可能なＩＣタグを備え、この包装材料と書籍、雑誌等を一体にすることにより、物流管理、返本管

理、万引き防止等の機能を備えることができる書籍、雑誌等の包装材料がある（例えば、特許文献２参照。）。

【特許文献１】特開平５－２６３５５８号公報

【特許文献２】特開２００２－３２６４７６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかし、上記特許文献２に記載の技術では、紙１枚単位の持ち出しを制限することは困難である。

【０００７】

そこで、本発明は、印刷物を紙１枚単位で持ち出しの制限を実施することで、文書等のセキュリティを高めることが可能な文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタを提供することを目的とする。

【課題を解決するための手段】

【０００８】

上記目的を達成するため、請求項１の発明は、クライアント装置からの印刷ジョブに基づき、プリンタが印刷した文書の文書持出制限システムにおいて、前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成する処理と、前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定する処理と、該設定した印刷ジョブを前記プリンタに送信する処理とをクライアント装置に動作させるプリンタドライバと、前記クライアント装置から受信した印刷ジョブを解析する印刷ジョブ解析手段と、前記印刷ジョブ解析手段で解析した印刷ジョブに設定されたセキュリティ情報を、前記用紙に付加されたＩＣタグに書き込むセキュリティ情報書込み手段と、前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを前記用紙に形成する印刷ジョブ処理手段とを具備するプリンタとを具備することを特徴とする。

【０００９】

また、請求項２の発明は、請求項１の発明において、前記用紙に付加されたＩＣタグに書き込まれたセキュリティ情報を読み込むセキュリティ情報読込手段と、前記セキュリティ情報読込手段で読み込んだセキュリティ情報に基づき、前記用紙が前記持出可能範囲への持出が許可されているか否か判定する判定手段とを具備し、前記持出可能範囲の境界に設置された検出器を更に具備することを特徴とする。

【００１０】

また、請求項３の発明は、請求項１の発明において、前記プリンタドライバは、前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する処理をクライアント装置に動作させることを特徴とする。

【００１１】

また、請求項４の発明は、クライアント装置からの印刷ジョブに基づき、プリンタが印刷した文書の文書持出制限方法において、前記クライアント装置のプリンタドライバは、前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成し、前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定し、該設定した印刷ジョブを前記プリンタに送信し、前記プリンタは、前記クライアント装置から受信した印刷ジョブを解析し、該解析した印刷ジョブに設定されたセキュリティ情報を、前記用紙に付加されたＩＣタグに書き込み、該解析した印刷ジョブに含まれる印刷データを前記用紙に形成することを特徴とする。

【００１２】

また、請求項５の発明は、請求項４の発明において、前記持出可能範囲の境界に設置された検出器は、前記用紙に付加されたＩＣタグに書き込まれたセキュリティ情報を読み込み、該読み込んだセキュリティ情報に基づき、前記用紙が前記持出可能範囲への持出が許可されているか否か判定することを特徴とする。

【００１３】
また、請求項６の発明は、請求項４の発明において、前記プリンタドライバは、前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定することを特徴とする。
【００１４】
また、請求項７の発明は、プリンタに送信する印刷ジョブを作成するクライアント装置にインストールされたプリンタドライバにおいて前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成する処理と、前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定する処理と、該設定した印刷ジョブを前記プリンタに送信する処理とをクライアント装置に動作させることを特徴とする。
【００１５】
また、請求項８の発明は、請求項７の発明において、前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する処理をクライアント装置に動作させることを特徴とする。
【００１６】
また、請求項９の発明は、クライアント装置と接続するプリンタにおいて、前記クライアント装置から受信した印刷ジョブを解析する印刷ジョブ解析手段と、前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を、該用紙に付加されたＩＣタグに書き込むセキュリティ情報書込み手段と、前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを前記用紙に形成する印刷ジョブ処理手段とを具備することを特徴とする。
【発明の効果】
【００１７】
本発明によれば、印刷物に対して、紙１枚単位で建物または建物のフロア毎にセキュリティを管理することが可能になるという効果を奏する。
【発明を実施するための最良の形態】
【００１８】
以下、本発明に係る文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタの実施の形態について添付図面を参照して詳細に説明する。なお、実施の形態として、ネットワークを介して本発明に係るプリンタとＰＣ［Personal Computer］等のクライアントとが接続し、クライアントに本発明に係るプリンタドライバがインストールされている構成を一例にして説明する。
【００１９】
図１は、本発明を適用した文書持出制限システム１の全体構成の一例を示すブロック図である。
【００２０】
図１に示すように、クライアント２とプリンタ３とがネットワーク４を介して接続している。なお、クライアント２－プリンタ３間をネットワーク４接続に限定する必要は無く、例えば、ＵＳＢ等のローカル接続の構成も適用可能である。
【００２１】
図１に示すように、クライアント２は、ＣＰＵ５、ＲＯＭ６、ＲＡＭ７、ＨＤ８、Ｉ／Ｆ９を具備して構成される。
【００２２】
ＣＰＵ［Central Processing Unit］５は、基本ソフトウェアであるオペレーティングシステム（以後、ＯＳと称する）に基づいてクライアント２本体のシーケンス制御を行なう。
【００２３】
ＲＯＭ［Read Only Memory］６は、クライアント２の起動時に実行されるプログラム等を記録する。

【0024】
ＲＡＭ［Random Access Memory］７は、プログラムの実行に必要なワークエリアのバッファエリアとして利用される。
【0025】
ＨＤ［Hard Disk］８は、ＯＳ、アプリケーションプログラム（以後、アプリケーションと称する）、プリンタドライバ、各種データ等を格納する。
【0026】
Ｉ／Ｆ［Interface］９は、ネットワーク４上のプリンタ３等の装置との間で各種データの送受信を行う。
【0027】
図２は、本発明に係るプリンタドライバ１０およびプリンタ３の機能的な構成の一例を示すブロック図である。
【0028】
図２に示すように、クライアント２には本発明に係るプリンタドライバ１０、および各種のアプリケーション１１がインストールされ、これらは、図示しないＯＳの制御下で、ＯＳの機能を利用して各種処理を実行する。また、ＰＣにはキーボードまたはマウス等の入力装置１２、ディスプレイ等の表示装置１３が接続されている。なお、前述したクライアント２に関する構成部以外の本発明と無関係な構成部についての説明は省略する。
【0029】
次に、プリンタドライバ１０の機能的な構成について説明する。
【0030】
図２に示すように、プリンタドライバ１０は、その機能として、印刷対象ファイル受付部１４、ＵＩ制御部１５、セキュリティ情報設定部１６、印刷情報設定部１７、印刷ジョブ作成部１８から構成される。
【0031】
印刷対象ファイル受付部１４は、アプリケーション１１から出力される文書、グラフィックまたは画像等の印刷対象ファイルを受け付ける処理を行う。
【0032】
ＵＩ制御部１５は、表示装置１３に表示するプリンタドライバＵＩ画面の表示制御の処理、入力装置１２から入力された印刷対象ファイルの印刷に関する印刷情報、用紙に埋め込まれたＩＣタグに書き込むセキュリティ情報等を受け付ける処理等を行う。
【0033】
セキュリティ情報設定部１６は、ＵＩ制御部１５で受け付けたセキュリティ情報を、印刷ジョブ作成部１８で作成する印刷ジョブに設定する処理を行う。ここで、セキュリティ情報とは、例えば、セキュリティの有無、持出可能範囲等の用紙持出制限を示す情報であり、印刷対象ファイルが複数の用紙で出力される場合は、各用紙毎にセキュリティ情報を設定することができる。例えば、１ページ目は持ち出しを許可し、２ページ目は事業所外への持ち出しを禁止し、３ページ目は建物外への持ち出しを禁止し、４ページ目はフロア外への持ち出しを禁止する、というように各ページ毎に持ち出し制限を設定することができる。
【0034】
印刷情報設定部１７は、ＵＩ制御部１５で受け付けた印刷情報を、印刷ジョブ作成部１８で作成する印刷ジョブに設定する処理を行う。
【0035】
印刷ジョブ作成部１８は、印刷対象ファイル受付部１４で受け付けた印刷対象ファイル、セキュリティ情報設定部１６で設定したセキュリティ情報、および印刷情報設定部１７で設定した印刷情報に基づいて印刷ジョブを作成する処理を行い、作成した印刷ジョブをＩ／Ｆ９を介してプリンタに送信する処理を行う。
【0036】
次に、プリンタ３の機能的な構成について説明する。

【0037】
図２に示すように、プリンタ３は、Ｉ／Ｆ９、印刷ジョブ解析部１９、セキュリティ情報書込み部２０、印刷ジョブ処理部２１を具備して構成される。なお、前述したプリンタ３に関する構成部以外の本発明と無関係な構成部についての説明は省略する。
【0038】
Ｉ／Ｆ９は、ネットワーク４上のクライアント２等の装置との間で各種データの送受信を行う。
【0039】
印刷ジョブ解析部１９は、クライアント２から受信した印刷ジョブを解析する処理を行う。
【0040】
セキュリティ情報書込み部２０は、印刷ジョブ解析部１９で解析した印刷ジョブに含まれるセキュリティ情報を、用紙２２に埋め込まれたＩＣタグ２３に書き込む処理を行う。
【0041】
印刷ジョブ処理部２１は、印刷ジョブ解析部１９で解析した印刷ジョブに含まれる印刷対象ファイルを印刷情報に従って画像に展開し、展開した画像を用紙２２上に形成する印字処理を行う。
【0042】
次に、印刷用紙にセキュリティ情報を書き込む際に行われるクライアント２およびプリンタ３の機能的な動作について図２を参照して説明する。
【0043】
ユーザが入力装置１２によりセキュリティ情報および印刷情報を入力し、クライアント２にインストールされたプリンタドライバ１０のＵＩ制御部１５は入力装置１２から入力されたセキュリティ情報および印刷情報を受け付け、セキュリティ情報をセキュリティ情報設定部１６に渡すとともに、印刷情報を印刷情報設定部１７に渡す。
【0044】
印刷対象ファイル受付部１４はアプリケーション１１から印刷対象ファイルを受け付けると、受け付けた印刷対象ファイルを印刷ジョブ作成部１８に渡し、印刷ジョブ作成部１８は印刷対象ファイルを受け取ると、受け取った印刷対象ファイルに基づいて印刷ジョブを作成し、作成した印刷ジョブに対し、セキュリティ情報指定部１６がセキュリティ情報を設定するとともに印刷情報設定部１７が印刷情報を設定し、印刷ジョブ作成部１８は印刷ジョブをＩ／Ｆ９を介してプリンタ３に送信する。
【0045】
プリンタ３の印刷ジョブ解析部１９は１／Ｆ９を介して受信した印刷ジョブを解析し、印刷ジョブに含まれたセキュリティ情報をセキュリティ情報書込み部２０に渡し、印刷ジョブに含まれた印刷対象ファイルおよび印刷情報を印刷ジョブ処理部２１に渡し、印刷ジョブ処理部２１は印刷対象ファイルおよび印刷情報を受け取ると、印刷情報に従って印刷対象ファイルの画像を用紙２２上に形成し、セキュリティ情報書込み部２０はセキュリティ情報を用紙２２に埋め込まれたＩＣタグ２３に書き込む。
【0046】
図３は、用紙２２に埋め込まれたＩＣタグ２３に書き込まれたセキュリティ情報を検出する検出器２４の機能的な構成の一例を示すブロック図である。
【0047】
図３に示すように、検出器２４は、所定の範囲に進入した用紙２２に埋め込まれたＩＣタグ２３に書き込まれたセキュリティ情報を読み込むセキュリティ情報読込部２５、この検出器２４に設定された持出制限の情報を格納する制限情報格納部２６、セキュリティ情報読込部２５が読み込んだセキュリティ情報と、制限情報格納部２６に格納されている持出制限の情報とを比較することにより用紙の持出許可／持出禁止を判定する判定部２７を具備して構成される。なお、判定部２７で持出禁止と判定した場合は警告出力装置２８が警告音等を出力し、用紙２２を持ち出そうとするユーザに対して注意を促す。

【0048】
次に、クライアントのプリンタドライバで行われる印刷用紙にセキュリティ情報を書き込む印刷ジョブを作成するための処理手順について図４に示すフローチャートを参照して説明する。
【0049】
アプリケーションから印刷対象ファイルを受け付け（ステップＳ４０１）、受け付けた印刷対象ファイルに基づいて印刷ジョブを作成し（ステップＳ４０２）、入力されたセキュリティ情報を受け付け（ステップＳ４０３）、受け付けたセキュリティ情報を印刷ジョブに設定し（ステップＳ４０４）、印刷ジョブをプリンタに送信し（ステップＳ４０５）、印刷ジョブを作成するための処理手順を終了する。
【0050】
次に、プリンタで行われる印刷用紙に埋め込まれたＩＣタグにセキュリティ情報を書き込むための処理手順について図５に示すフローチャートを参照して説明する。
【0051】
クライアントから印刷ジョブを受信し（ステップＳ５０１）、受信した印刷ジョブを解析し（ステップＳ５０２）、印刷ページを表す「ｎ」を「０」に設定し（ステップＳ５０３）、「ｎ」に「１」を加算し（ステップＳ５０４）、印刷ジョブに含まれたｎページ目の画像を用紙上に形成し（ステップＳ５０５）、印刷ジョブに含まれたセキュリティ情報を用紙に埋め込まれたＩＣタグに書き込み（ステップＳ５０６）、ｎページ目が最終ページではない場合（ステップＳ５０７でＮＯ）、ステップＳ５０４に戻り、また、ｎページ目が最終ページである場合（ステップＳ５０７でＹＥＳ）、ＩＣタグにセキュリティ情報を書き込むための処理手順を終了する。
【0052】
次に、検出器で行われるＩＣタグから読み込んだセキュリティ情報に基づいて用紙持ち出しの許可／禁止を判定するための処理手順について図６に示すフローチャートを参照して説明する。
【0053】
所定の範囲に進入した用紙に埋め込まれたＩＣタグからセキュリティ情報を読み込み（ステップＳ６０１）、セキュリティ情報と制御情報とに基づいて持出制限を判定し（ステップＳ６０２）、持出禁止の場合（ステップＳ６０３でＹＥＳ）、ステップＳ６０４に進み、また、持出許可の場合（ステップＳ６０３でＮＯ）、持出の許可／禁止を判定するための処理手順を終了する。
【0054】
持出禁止の場合（ステップＳ６０３でＹＥＳ）、警告出力装置に警告を出力するように指示し（ステップＳ６０４）、持出の許可／禁止を判定するための処理手順を終了する。
【0055】
図７は、本発明に係る用紙持出制限方法の具体例を示す図である。
【0056】
図７に示すように、複数の用紙で構成されている文書があり、各用紙毎にＩＣタグが埋め込まれ、そのＩＣタグには、「任意の範囲（例えば、部屋、フロア、建物等）の中での異動は可能」、「その任意の範囲外への持出は禁止」というセキュリティ情報が書き込まれ、その任意の範囲外へ出る出口には検出器および警告出力装置が設置されている。
【0057】
従って、その文書のうち１枚の用紙を人が範囲外に持ち出そうとしても、出口に設置された検出器が、持ち出そうとする１枚の用紙のＩＣタグに書き込まれたセキュリティ情報に基づいてその用紙が持出禁止の用紙であることを判定し、警告出力装置から警告音等が出力される。
【0058】
このように、用紙１枚単位で持出許可／禁止の管理を行うことで、例えば、スーパーマーケット、百貨店、小売店等の店舗における商品の万引きまたは盗難を防止する以外にも

、図書館の本のページを破いて持ち出す行為。会社に保管された文書の中から機密情報が記載された用紙のみを持ち出す行為等も防止することが可能になる。

【0059】

また、図８に示すように、特別な事情があって任意の範囲外に用紙を持ち出さなければならない場合、その用紙の持出を許可する情報をＩＣタグに書き込んだ持出許可用紙２９を、本発明に係るプリンタドライバおよびプリンタで印刷し、その持出許可用紙２９と持出用紙とを一緒に持つことで、検出器が持出用紙の持出を許可し、警告出力装置から警告音等が出力されないような構成も可能である。

【0060】

なお、本発明の実施の形態として、クライアントにインストールされたプリンタドライバが印刷ジョブにセキュリティ情報を設定する構成を一例に説明したが、本発明はこのような構成に限定する必要は無く、例えば、プリンタのコントロールパネル等でセキュリティ情報を入力し、プリンタがそのセキュリティ情報を用紙のＩＣタグに書き込む構成も適応可能であり、更に、このようなセキュリティ情報を書き込むことが可能なコピー機も適応可能である。

【図面の簡単な説明】

【0061】

【図１】本発明を適用した文書持出制限システムの全体構成の一例を示すブロック図である。

【図２】本発明に係るプリンタドライバおよびプリンタの機能的な構成の一例を示すブロック図である。

【図３】用紙に埋め込まれたＩＣタグに書き込まれたセキュリティ情報を検出する検出器の機能的な構成の一例を示すブロック図である。

【図４】クライアントのプリンタドライバで行われる印刷用紙にセキュリティ情報を書き込む印刷ジョブを作成するための処理手順を示すフローチャートである。

【図５】プリンタで行われる印刷用紙に埋め込まれたＩＣタグにセキュリティ情報を書き込むための処理手順を示すフローチャートである。

【図６】検出器で行われるＩＣタグから読み込んだセキュリティ情報に基づいて用紙持ち出しの許可／禁止を判定するための処理手順を示すフローチャートである。

【図７】本発明に係る用紙持出制限方法の具体例を示す図である。

【図８】持出許可用紙を説明する図である。

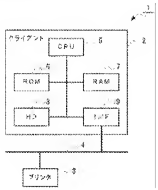
【符号の説明】

【0062】

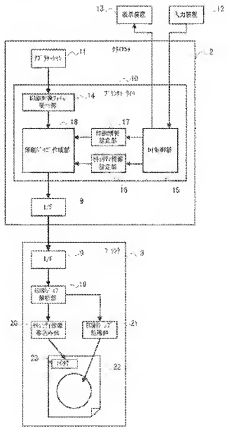
１　文書持出制限システム
２　クライアント
３　プリンタ
４　ネットワーク
５　ＣＰＵ
６　ＲＯＭ
７　ＲＡＭ
８　ＨＤ
９　Ｉ／Ｆ
１０　プリンタドライバ
１１　アプリケーション
１２　入力装置
１３　表示装置
１４　印刷対象ファイル受付部
１５　ＵＩ制御部
１６　セキュリティ情報設定部
１７　印刷情報設定部

１８　印刷ジョブ作成部
１９　印刷ジョブ解析部
２０　セキュリティ情報書込み部
２１　印刷ジョブ処理部
２２　用紙
２３　ＩＣタグ
２４　検出器
２５　セキュリティ情報読込部
２６　制限情報格納部
２７　判定部
２８　警告出力装置
２９　持出許可用紙

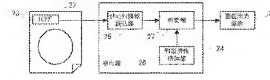
【図1】



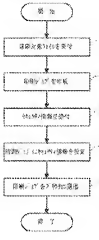
【図2】



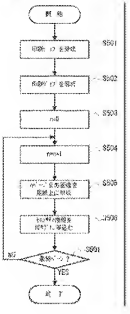
【図３】


ICタグ
セキュリティ情報読込部
判定部
警告出力装置
特定情報保存装置
記憶部

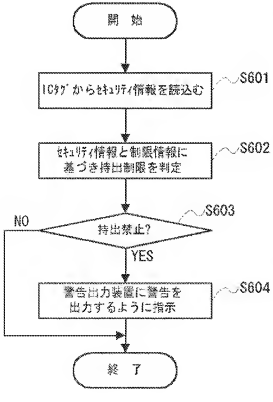
【図４】


開　始
S401
S402
S403
S404
S405
終　了

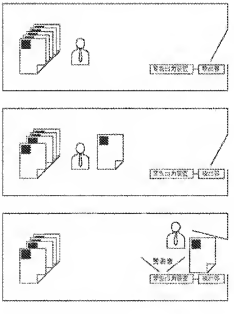
【図５】


開　始
S501
S502
S503
S504
S505
S506
S507
NO
YES
終　了

【図６】


開　始
ICタグからセキュリティ情報を読込む
S601
セキュリティ情報と制限情報に
基づき持出制限を判定
S602
持出禁止?
S603
NO
YES
警告出力装置に警告を
出力するように指示
S604
終　了

【図７】


警告出力装置
物品番
警告出力装置
物品番
禁止物
警告出力装置
物品番

【図８】